



State of Illinois
Department of Central Management Services

DATA CLASSIFICATION

Standard

Effective January 30, 2007

Public Distribution

Version 1.0

DATA CLASSIFICATION

Effective January 30, 2007

Version 1.0

APPROVAL SHEET

EXPEDITED APPROVAL

BCCS Deputy Director: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Owner: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Policy Review Board Chair: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Return to Policy Review Board Chair

Expedited publications MUST be formally submitted to the Policy Review Board within 180 days from the BCCS Deputy Director approval date in order to undergo customary review and stakeholder comment or the publication will be withdrawn and retired.

Illinois Department of Central Management Services (CMS)
DATA CLASSIFICATION STANDARD

IDENTIFICATION

This standard establishes the criteria for classifying data and information into three categories of confidential, sensitive, and public. This classification applies to the data only and not to the tool which eventually displays the information. As an example, Outlook is a tool that reads an email file and displays the data onto a computer screen or prints the message into a hardcopy version. This classification applies to the file, not to Outlook or to the computer monitor or to the printer. If, however, information displayed is confidential, then precautions must be taken to protect its unauthorized view regardless of the method in which it is displayed.

AUTHORITY

This standard implements the requirements of the CMS Security Policy which states that a data classification hierarchy be established to delineate proper protection procedures. In addition, this standard meets the best practice recommendations of NIST and ISO 17799.

AUDIENCE

This classification applies to all data maintained on CMS managed devices.

The impact of this standard could be significant. Implementation will require that every data file be examined in order to identify the level of security needed and thus a classification applied. An additional procedure must be established to accommodate a change that reclassifies a particular file. For example, if a law passes that protects a person's wage information, then payroll files must be reclassified from sensitive to confidential and additional controls applied to those files containing wage information.

Illinois Department of Central Management Services (CMS)
DATA CLASSIFICATION STANDARD

DATA CLASSIFICATION STANDARD

Please note that data and information are synonymous in the descriptions below and are used interchangeably to mean the same thing.

Classification is important because it determines the level of security to be applied to the data, the application that processes the data, and the environment which houses/stores the data. As would be expected, confidential data requires the most stringent security, sensitive requires less control than confidential but more control than public, while public data requires very little security (only controls over the integrity of the data are necessary). Classification can be determined by the following:

CONFIDENTIAL	SENSITIVE	PUBLIC
Any information that if lost, corrupted, or disclosed to or accessed by an unauthorized person may cause harm, injury, damage, or significant financial loss to another person or entity or which may corrupt the organization's mission.	Any information that if lost, corrupted, or disclosed to or accessed by an unauthorized person may cause embarrassment, humiliation, or dishonor to another person or entity.	Any information that if lost or disclosed to or accessed by any individual will, without question, <u>not</u> harm, damage, hurt, embarrass, humiliate, dishonor, or cause financial loss to another person or entity.
Any information that is excluded from Freedom of Information disclosure that meets criteria as defined in Section 7, Exemptions, of the Freedom of Information Act (5 ILCS 140/)	Any information that is explicitly referenced in the Freedom of Information Act (5 ILCS 140/) as requiring completion of a formal request prior to release to the requesting individual.	Any information that is explicitly identified in the Freedom of Information Act (5 ILCS 140/) as not requiring a formal request prior to publication accessible by the general public.
All protected health information as defined by HIPAA		
Information containing personal, private data on employees, contractors, or clients.		
Information that if disclosed or accessed by unauthorized means or persons or if lost or corrupted would violate state or federal law.		

Illinois Department of Central Management Services (CMS)
DATA CLASSIFICATION STANDARD

REVISION HISTORY

Created: May 1, 2006
Revised: Nov 17, 2006 / Jun 15, 2006 / Dec 18, 2006
Reviewed: Nov 17, 2006
Effective: Jan 30, 2007

- End of Data Classification Standard -